



Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 311

[Docket ID: DoD-2015-OS-0077]

Privacy Act of 1974; Implementation

AGENCY: Office of the Secretary, DoD.

ACTION: Direct final rule with request for comments.

SUMMARY: The Office of the Secretary of Defense (OSD) is exempting those records contained in DPFPA 07, entitled "Counterintelligence Management Information System (CIMIS)," pertaining to investigatory material compiled for counterintelligence and law enforcement purposes (under (k)(2) of the Act), other than material within the scope of subsection (j)(2) of the Privacy Act to enable the protection of identities of confidential sources who might not otherwise come forward and who furnished information under an express promise that the sources' identity would be held in confidence. The exemption will allow DoD to provide protection against notification of investigatory material including certain reciprocal investigations which might alert a subject to the fact that an investigation of

that individual is taking place, and the disclosure of which would weaken the on-going investigation, reveal investigatory techniques, and place confidential informants in jeopardy who furnished information under an express promise that the sources' identity would be held in confidence. Further, requiring OSD to grant access to records and amend these records would unfairly impede the investigation of allegations of unlawful activities. To require OSD to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

DATES: The rule will be effective on December 9, 2015 unless adverse comments are received by [INSERT DATE 60 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER]. If adverse comment is received, the Department of Defense will publish a timely withdrawal of the rule in the Federal Register.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

- Federal Rulemaking Portal:
<http://www.regulations.gov>. Follow the instructions for submitting comments.
- Mail: Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, Regulatory and Audit Matters Office, 9010 Defense Pentagon, Washington, DC 20301-9010.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Cindy Allard at (571) 372-0461.

SUPPLEMENTARY INFORMATION:

This direct final rule makes changes to the Office of the Secretary Privacy Program rules. These changes will allow the Department to add an exemption rule to the Office of the Secretary of Defense Privacy Program rules that will exempt applicable Department records and/or material from certain portions of the Privacy Act.

This rule is being published as a direct final rule as the Department of Defense does not expect to receive any adverse comments, and so a proposed rule is unnecessary.

Direct Final Rule and Significant Adverse Comments

DoD has determined this rulemaking meets the criteria for a direct final rule because it involves non-substantive changes dealing with DoD's management of its Privacy Programs. DoD expects no opposition to the changes and no significant adverse comments. However, if DoD receives a significant adverse comment, the Department will withdraw this direct final rule by publishing a notice in the Federal Register. A significant adverse comment is one that explains: (1) Why the direct final rule is inappropriate, including challenges to the rule's underlying premise or approach; or (2) why the direct final rule will be ineffective or unacceptable without a change. In determining whether a comment necessitates withdrawal of this direct final rule, DoD will consider whether it warrants a substantive response in a notice and comment process.

Executive Order 12866, "Regulatory Planning and Review" and Executive Order 13563, "Improving Regulation and Regulatory Review"

It has been determined that Privacy Act rules for the Department of Defense are not significant rules. This rule does not (1) Have an annual effect on the economy of \$100 million or more or adversely affect in a material way the economy; a sector of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities; (2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency; (3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or (4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in these Executive orders.

Public Law 96-354, "Regulatory Flexibility Act" (5 U.S.C Chapter 6)

It has been determined that this Privacy Act rule for the Department of Defense does not have significant economic impact on a substantial number of small entities because it is concerned only with the administration of Privacy Act systems of records within the Department of Defense. A Regulatory Flexibility Analysis is not required.

Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C.

Chapter 35)

It has been determined that this Privacy Act rule for the Department of Defense imposes no information requirements beyond the Department of Defense and that the information collected within the Department of Defense is necessary and consistent with 5 U.S.C. 552a, known as the Privacy Act of 1974.

Section 202, Public Law 104-4, "Unfunded Mandates Reform Act"

It has been determined that this Privacy Act rule for the Department of Defense does not involve a Federal mandate that may result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of \$100 million or more and that this rulemaking will not significantly or uniquely affect small governments.

Executive Order 13132, "Federalism"

It has been determined that this Privacy Act rule for the Department of Defense does not have federalism implications. This rule does not have substantial direct effects on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of

government. Therefore, no Federalism assessment is required.

List of Subjects in 32 CFR Part 311

Privacy.

Accordingly, 32 CFR part 311 is amended to read as follows:

PART 311-OFFICE OF THE SECRETARY OF DEFENSE AND JOINT STAFF PRIVACY PROGRAM

1. The authority citation for 32 CFR part 311 continues to read as follows:

Authority: 5 U.S.C. 522a.

2. Section 311.8 is amended by adding paragraph (c) (25) to read as follows:

§ 311.8 Procedures for exemptions.

* * * * *

(c) * * *

(25) System identifier and name: DPFPA 07,
Counterintelligence Management Information System (CIMIS).

(i) Exemptions: Portions of this system that fall within 5 U.S.C. 552a (k) (2) are exempt from the following provisions of 5 U.S.C. 552a, section (c) (3); (d); (e) (1); (e) (4) (G) through (I); and (f) of the Act, as applicable.

(ii) Authority: 5 U.S.C. 552a (k) (2).

(iii) Reasons:

(A) From subsections (c)(3) because making available to a record subject the accounting of disclosure from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected offender by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(B) From subsection (d) because these provisions concern individual access to and amendment of certain records contained in this system, including counterintelligence, law enforcement, and investigatory records. Compliance with these provisions could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of agencies; compromise sensitive information related to national security; interfere with the overall counterintelligence and investigative process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a

confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigation or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses.

Amendment of these records would interfere with ongoing counterintelligence investigations and analysis activities and impose an excessive administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(C) From subsection (e)(1) because it is not always possible to determine what information is relevant and necessary at an early stage in a given investigation. Also, because Pentagon Force Protection Agency and other agencies may not always know what information about a known or suspected offender may be relevant to for the purpose of conducting an operational response.

(D) From subsections (e)(4)(G) through (I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(E) From subsection (f) because requiring the Agency to grant access to records and establishing agency rules for amendment of records would compromise the existence of any criminal, civil, or administrative enforcement activity.

To require the confirmation or denial of the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to the existence of an on-going investigation.

Counterintelligence investigations would be jeopardized by agency rules requiring verification of the record, disclosure of the record to the subject, and record amendment procedures.

Dated: July 31, 2015.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2015-24791 Filed: 9/29/2015 08:45 am; Publication Date: 9/30/2015]